UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF FOUR EMAIL ACCOUNTS STORED AT PREMISES CONTROLLED BY GOOGLE, LLC PURSUANT TO 18 U.S.C. § 2703 FOR INVESTIGATION OF VIOLATIONS OF 18 U.S.C. §§ 201, 371, 1001, 1343, 1546, 1956, and 31 U.S.C. § 5324	**21-mj-**282-01/04-AJ **Filed Under Seal**

Subject Accounts: orlandoclark8@gmail.com, wmsconstructiondesign@gmail.com, raj.wafi@gmail.com, aufcc.company@gmail.com

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Kevin Naylon, the undersigned Affiant, being first duly sworn, hereby state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information which is associated with four email accounts – that is, orlandoclark8@gmail.com ("**SUBJECT ACCOUNT #1**"), wmsconstructiondesign@gmail.com ("**SUBJECT ACCOUNT #2**"), raj.wafi@gmail.com ("**SUBJECT ACCOUNT #3**"), and aufcc.company@gmail.com (**SUBJECT ACCOUNT #4**) – which are stored at premises controlled by Google, LLC ("PROVIDER"), an electronic communications services provider and/or remote computing services provider which is located at 1600 Amphitheatre Parkway, Mountain View, CA 94043 (collectively, the "**SUBJECT ACCOUNTS**"). The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require PROVIDER to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information

described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, using the procedures described in Section III.

2. I am a Special Agent with Special Inspector General for Afghanistan Reconstruction ("SIGAR"). I have been in this position since July 2012. Before joining SIGAR, I was a Special Agent with the U.S. Naval Criminal Investigative Service for nearly 24 years. I have conducted investigations regarding white collar crime concerning violations of federal law. The investigations include, but are noted limited to, fraud against the government, theft of government property, wire and mail fraud, and money laundering. I possess an undergraduate degree in public administration from Virginia Commonwealth University.

3. The facts in this affidavit come from my personal observations, training, experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all my knowledge, or the knowledge of others, about this matter. All dates alleged herein are alleged to be "on or about" the dates stated.

4. Based on my training and experience and the facts in this affidavit, I submit that there is probable cause to believe that violations of 18 U.S.C. § 201 (Bribery), § 371 (Conspiracy), § 1001 (False Statement), § 1343 (Wire Fraud), § 1546 (Visa Fraud), § 1956 (Money Laundering), and 31 U.S.C. § 5324 (Structuring) have been committed. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction because it is a "court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). As discussed below, acts or omissions in furtherance of the scheme under investigation occurred in the District of New Hampshire. *See* 18 U.S.C. § 3237.

PROBABLE CAUSE

6. In September 2020, the U.S. Department of State received a complaint alleging a U.S. servicemember, Jeromy Pittman ("Pittman"), who was the complainant's supervisor, had been bribed by Afghan companies and conspired with an Afghan citizen, Ghullam Jan Daler ("Daler"), to write false recommendation letters for Afghans applying for Special Immigrant Visas ("SIVs").[1]

7. On August 19, 2021, this Court granted an application for a search warrant for an email account which Pittman had listed on SIV letters that he allegedly wrote, and which he used to falsely verify such letters when responding to inquiries from the U.S. Department of State, National Visa Center, located in the District of New Hampshire (Case No. 21-MJ-209-01-AJ).

8. The complainant also described activity of another U.S. citizen, Orlando Clark ("Clark"), who allegedly helped award contracts to Afghan companies in exchange for bribes, and who was thereafter bribed to sign SIV letters. Like Pittman, the allegations as to Clark have been corroborated by records and interviews discussed herein. Your Affiant will discuss: (A) the SIV scheme involving Pittman and Daler; (B) the procurement fraud scheme involving Clark and an Afghan company that appears to be owned by Daler's relative; and (C) the SIV scheme involving Clark and Afghan companies.

[1] Federal law authorizes a limited supply of SIVs each year to Iraqi and Afghan interpreters who have worked for the U.S. military or who have worked for or on behalf of the U.S. government in Iraq or Afghanistan.

A. <u>The SIV Scheme Involving Pittman and Daler</u>

9. The complaint alleges that Pittmann had been receiving bribe payments for writing letters from, among other entities, a construction company in Afghanistan named Sunny Universe, which is controlled, in part, by Daler, a citizen of Afghanistan residing in the United Kingdom.

10. The complaint also alleges that emails were sent in furtherance of the scheme:

> From 2016 to present Mr Jan made a secret network with the US GOV former Am[e]rican supervisors whom [] worked w[ith] him in his contracts[.] [A]s [] supervisors they were very near[], close[] [sic] friends with Mr[.] Ghullam Jan in the project sites while his contracts were under performance[.] [T]hese US GOV Am[e]rican supervisors [] names are JERMMY [sic] PITTMANN CPT and Mr Mathew Attorn[.] [*T]hese Am[e]ricns are now working with him through secret link[s] as well as WHATS UP and private emails with him[.]* [T]hese Am[e]rican soldiers [s]igned recommend[ation] letters for him against money for each applicant[.] [H]e pay to each supervisor around 1000$ thru [sic] his secret agents now in the USA CLF City[.] . . .
>
> When the embassy request confirmation from the Am[e]rican *[t]hat supervisor forwarded the email to GHULLAM JAN DALER*[.] [H]e checked his record then he say to the rec[]ommender [p]lease confirm he is good[.]
>
> Then the Am[e]rican whom he bribed thru [sic] Jan NETWORK he confirmed to the embassy yes I gave him this letter he worked under his supervision on this location as a[n] interpreter or for[e]man or other any skill that written to his HR letter. (emphasis added).

11. In investigating the allegations, your Affiant has obtained and reviewed records from the U.S. Departments of State and Defense, which appear to corroborate the complaint. Records show that Pittmann is a Commander in the U.S. Navy Reserve, in which capacity he wrote 21 letters of recommendation between May 2018 and September 2020.

12. The 21 letters Pittman signed appear to use the same boilerplate description for each applicant (i.e., the applicant "worked in support of United States army and NATO forces," was "a diligent, polite and hardworking individual" and did not pose "a threat to the national security or safety of the United States of America," among other things).

13. The SIV applications including Pittmann's letter were accompanied by separate letters from Sunny Universe, which appear to be written and signed by Ghulman Qaderi.[2]

14. Emails obtained from Pittmann's personal account pursuant to a search warrant issued by this Court reflect that Pittmann coordinated with Daler in drafting fraudulent SIV letters, verifying such letters in response to inquiries from the National Visa Center, and receiving bribes.

15. For example, On February 3, 2018, Pittman received an email from the account listed on all Sunny Universe letters supporting SIV applicants, which appears to have been used by Daler (sunnycc.company@gmail.com). The email stated: "I have been contacted some people they needed a recommendation letter from an American supervisor or engineer or COR. Do you think you can write them a recommendation letter for SIV? They will pay for it." The signature block in the email listed "Ghulam Rabani" which appears to be another name that Daler uses. Pittmann replied, "Who is this for?" Daler replied: "It's for my cousins I have 5 of them to go if you can do it will be good and they will pay for it." Pittmann replied: "How much is he paying?" After some back and forth, Daler replied: "500 each so it's 3 of them total will be 1500 [a]n[d] other 2 end of this week will bring their ID so it will be another 100 I will have another 5 next week so will be 2500. [Don't] forget my sweet as well[.]" Pittmann replied, "Send me the info." Thereafter, consistent with the complaint, Daler wire transferred funds to an agent in California, who then wired the funds to Pittman.

16. Accordingly, your Affiant believes—consistent with allegations in the complaint, and consistent with the corroborative evidence your Affiant has obtained in this investigation—that other Afghan companies discussed in the complaint similarly coordinated with individuals, such as Clark, by using email accounts in furtherance of the schemes, discussed below.

---

[2] Daler and Ghulman Qaderi appear to be the same person based on evidence obtained in the investigation, including a British passport.

B. The Procurement Fraud Scheme Appears to Involve Clark and Daler's Relative

17. As to the scheme involving Clark, the complaint states the following:

> Mr[.] Qazafi Samadi Son [o]f Mohmmad Rabani from Panjshir province AFGHANISTAN[.] [H]e is the owner for the RAJ CONSTRUCTION CO[.] [T]his company worked multiple contracts under the direct supervise [sic] of ORLANDO CLARK in Helmand province Afghanistan. Mr[.] Samadi paid around $900,000.00 to him thru [sic] his HAWALA [Afghan system to transfer money]. Mr Clark was sent the money to his wife . . .
>
> He many times came to Dubai through USA met with the three companies [sic] owners & he got his money in Dubai[.] [T]otal money he got from three companies were around 1,800,000 $$$$ from 35 directly awarded contracts through Orlando Clark at dawyer [sic] contracting office or Leathernick [sic] contracting office in Helmand province AFG . . .
>
> Trust me for each project Mr Orlando paid around 20 % of those contracts in the partial payments when they rcvd [sic] . . .
>
> QAZAFI Samadi Son of Mohammad [R]abani owner for **RAJ CONSTRUCTION** he was the main facilitator to Mr Clark on three companies[.]

18. Government records indicate that around July 2011, an Afghan company, Raj Construction ("Raj"), owned by Qazafi Samadi ("Samadi"), began bidding on U.S. government contracts; that in November 2011, Clark, a contractor with URS Group, Inc., deployed to Afghanistan to perform construction management services; and that Todd Coleman ("Coleman"), a contractor with CACI International, Inc. who potentially conspired with Clark, deployed in 2011.

19. Contract records indicate that in 2012, Raj received at least four contracts for $889,000, $888,000, $620,000, and $36,000 (around $2.4 million). The two larger contracts (for approximately $1.8 million, which is consistent with the complaint) involved construction of an Afghan police station and security check point to be used by U.S. forces. Coleman is listed on records as a Contract Administrator. He also signed documents justifying in the interest of national security contracts to only Afghan companies, indicating he potentially attempted to steer contracts. Records also reflect that Coleman communicated, via email, with the owner of Raj, Samadi.

20. Consistent with the complaint, Clark and Raj appear to have potentially conspired to structure the transfer of bribes in furtherance of a scheme to obtain contracts. For example, on June 27, 2012, while deployed, Clark wired approximately $5,000 to his wife in Atlanta, Georgia, through Western Union in Dubai, United Arab Emirates. Then, approximately six minutes later, "Qazafi So [son of] Ghulam Rabani" who, based on the complaint, appears to be the owner of Raj, wired approximately $5,000 to Clark's wife from the same Western Union station that Clark used.[3]

21. Also consistent with the complaint, Clark began flying between Dubai and Atlanta: four days after the latter wire (July 1, 2012), he flew from Dubai to Atlanta; about two weeks later, he flew from Atlanta to Dubai; while abroad, his deployment ended, after which he wired approximately $4,000 to his wife; Clark returned to Atlanta two weeks later (August 15, 2012).

22. Two days after returning to Atlanta (August 17, 2012), Clark used his home address in Georgia to register Raj Premier International, LLC ("Raj International"), into which Raj potentially laundered bribes. Records obtained indicate Clark and Coleman organized the LLC.[4]

23. Five days later, Coleman issued Clark two wires from Dubai for $9,000.

24. Bank records reflect that one week later (August 31, 2012), Clark and Coleman opened a business bank account in the name of Raj International.

25. The next month (September 2012), it appears that a Raj employee (Mohammad Hussain Hussaini, a SIV applicant discussed below) wired Clark around $5,000 from Afghanistan.

26. Also in September 2012, an Afghan company affiliated with Raj, Raj Premier Logistic Services Company ("Raj Logistic"), began operations based on government records.

---

[3] As discussed above, "Ghulam Rabani" is the name potentially used by Daler (see Paragraph 15). As such, Daler appears to own Sunny Universe, and his relative (and possibly his son), Samadi, appears to own Raj.

[4] Records obtained in the investigation indicate that a company named "Raj Premier Investments" was also registered in Dubai in 2012. We are investigating whether the entities are related.

27. Over the course of about seven months, between September 2012 and April 2013, Raj Logistic sent, through 22 wires from Afghanistan, around $255,000 to entities linked to Clark, which approximates 10% of the value of the contracts discussed above that were awarded to Raj:

	Date	Amount	Originator	Beneficiary	Wire Reference
1	9-17-12[5]	$89,965	Raj Logistic	Raj International	Payment for Vehicles
2	10-4-12	$9,870	Raj Logistic	Raj International	Bills Operating Expenses
3	10-15-12[6]	$7,152	Raj Logistic	Raj International	Bills Operating Expenses
4	10-22-12	$9,870	Raj Logistic	Raj International	Goods Purchase
5	10-31-12	$9,870	Raj Logistic	Raj International	Goods Purchase
6	11-8-12	$9,870	Raj Logistic	Raj International	Bills Operating Expenses
7	11-13-12[7]	$9,870	Raj Logistic	Raj Investments	Purchase Investment
8	11-20-12	$9,870	Raj Logistic	Raj Investments	Bills Operating Expenses
9	11-27-12	$9,870	Raj Logistic	Raj Investments	Goods Purchase
10	11-29-12	$9,870	Raj Logistic	Raj Investments	Goods Purchase
11	12-4-12	$9,870	Raj Logistic	Raj Investments	Bills Operating Expenses
12	12-6-12	$9,870	Raj Logistic	Raj Investments	Goods Purchase
13	12-10-12	$9,870	Raj Logistic	Raj Investments	Bills Operating Expenses
14	12-17-12	$9,870	Raj Logistic	Raj Investments	Goods Purchase
15	12-24-12	$9,870	Raj Logistic	Raj Investments	Bills Operating Expenses
16	1-7-13	$2,975	Raj Logistic	Raj Investments	Bills Operating Expenses
17	1-22-13	$7,790	Raj Logistic	Raj Investments	Bills Operating Expenses
18	1-30-13[8]	$4,975	Raj Logistic	Raj Investments	Bills Operating Expenses
19	2-7-13	$5,970	Raj Logistic	Raj Investments	Bills Operating Expenses
20	3-11-13	$500	Raj Logistic	Raj Investments	Bills Operating Expenses
21	4-15-13	$6,970	Raj Logistic	Raj Investments	Bills Operating Expenses
22	4-24-13	$445	Raj Logistic	Raj Investments	Bills Operating Expenses

[5] One week later (September 25, 2012), Clark flew to Dubai. While abroad, Raj Logistic remitted a second wire for $9,900 after which he returned to Atlanta five days later (October 9, 2012). Given the discrepancy between the first wire for $90,000, and the subsequent wires that were barely beneath the $10,000 threshold for bank reporting, it is possible, based on my training and experience, that Clark may have advised Raj Logistic not to wire amounts exceeding $10,000 in order to conceal the criminal activity based on the mistaken belief that the reporting requirement is triggered by wires, although it only applies to cash. Bank records reflect that when asked to explain the purpose and reason for the pattern of transactions, Raj stated that the reason "is for Bill Operating expenses and payment for purchase of goods," which did not answer the question. Your Affiant further notes that Coleman may have travelled to Dubai for the same purpose as Clark; he flew to Dubai five days after Clark (September 30, 2012) and returned to the United States one day after Clark (October 10, 2012).

[6] On this date, Clark and Coleman opened a second bank account in the name of Raj International.

[7] Five days before this wire, Clark used his home address to register Raj Premier Investments, LLC ("Raj Investments"); the next day he opened a third bank account into which subsequent wires from Raj were remitted.

[8] On this date, Clark flew back to Dubai and returned to Atlanta 10 days later. He thereafter flew back to Dubai three more times between the rest of 2013 and 2014.

28. Evidence obtained indicates that Raj Logistic had represented to Afghanistan International Bank (from which the wires were sent to the United States) that the purpose of the transactions was "payment to the mother company in USA for Bills operating expenses." Yet it appears a substantial portion of funds were withdrawn for personal rather than business expenses, such as "David Yurman" (jewelry) and "Luis Vuitton" (clothes), among other personal expenses.[9]

29. Based on the foregoing, your Affiant believes that the wires were potentially bribes, which Clark laundered through personal purchases, all of which is consistent with the complaint:

30. Also consistent with the complaint, Western Union records reflect that Clark and his wife received wires from Afghanistan in amounts consisting of (or close to) $5,000:

a. On September 6, 2014, Mohammad Saleh Mohammad Nabi wired Clark $5,000 from Afghanistan to his home address (used to register the Raj LLCs in Georgia); five days later, Clark flew to Dubai; he returned 10 days later (September 21, 2014); on November 5, 2014, Mohammad Saleh Mohammad Nabi wired Clark $5,000 from Afghanistan to the same address; 10 days later, Clark flew to Dubai.

b. While Clark was abroad, Qazafi Ghulam Rabani wired Clark's wife $5,000 from Afghanistan (November 27, 2014); two days later, Mohammad Salih wired Clark's wife $4,500 from Afghanistan; five days later, Clark returned to Atlanta.[10]

31. In May 2015, Clark filed a notice to dissolve Raj International and Raj Investments. Further consistent with the complaint, which alleges that after the procurement fraud scheme ended Afghan company owners threatened to report Clark to SIGAR unless he signed SIV letters, he appears to have started signing SIV letters approximately six months after dissolving the Raj LLCs.

---

[9] The bank records further indicate that the withdrawals are potentially connected to Coleman. For example, on October 25, 2012, the Raj Premier statement indicates there was a $20,034 withdrawal from a Wells Fargo branch. A currency transaction report was filed indicating Coleman withdrew the funds and then made a deposit the same day in an account in the name of Lano USA, Inc., which appears to be a used car dealer in Georgia.

[10] "Qazafi Ghulam Rabani" appears to indicate the wire was from Raj and further links Daler to Samadi. Moreover, contract records for Raj lists a phone number of "0093777140190" and the Western Union number is "930777140190" (which appears to be the same but with a zero-digit before the country code for Afghanistan, 93). As to the other three wires, contract records further indicate a man named "Muhammad Saleh" was a manager at Raj.

C. The SIV Scheme Involving Clark and Samadi

a. Clark's SIV Letters (SUBJECT ACCOUNTS #1 and #2)

32. Consistent with the complaint, Clark appears to have signed at least 12 SIV letters:

	Applicant	Date of Clark's Letter
1	Mohammad Farooq Amin	10-18-15
2	Maitullah Hamidi	6-13-16
3	Tamim Amiri	6-13-16
4	Habib Ruhman	7-6-16
5	Abdul Hamed Qadiri	7-25-16
6	Mohammad Qais	9-5-16
7	Mir Anayatullah	11-27-16
8	Qazafi Samadi	11-7-17
9	Akhtar Mohammad	10-7-18
10	Mohammad Islam Safa	10-7-18
11	Mohammad Hussain Hussaini	10-7-18
12	Azatullah Nazari	2-18-19

The above letters indicate that **SUBJECT ACCOUNT #1** is Clark's email account. Furthermore, the first letter for Amin also indicates that **SUBJECT ACCOUNT #2** is Clark's email account.

33. Clark also used **SUBJECT ACCOUNT #2** (as well as his passport) to reply to the National Visa Center when verifying letters (Nazari, Samadi, Hussaini, Amin, Anayatullah, Safa). Furthermore, he copied **SUBJECT ACCOUNT #1** when verifying a letter (Amin).

34. The veracity of the letters, however, is belied by inconsistencies between the dates during which Clark supervised applicants and his term of deployment listed in government records.

	Applicant	Dates of Supervision	Clark's Deployment
1	Maitullah Hamidi	Jan. 2010-Jan. 2011	Oct. 2011-Aug. 2012
2	Azatullah Nazari	Jan. 2010-Jan. 2011	Oct. 2011-Aug. 2012
3	Tamim Amiri	Jan. 2010-Jan. 2011	Oct. 2011-Aug. 2012
4	Habib Ruhman	Jan. 2010-Jan. 2011	Oct. 2011-Aug. 2012
5	Abdul Hamed Qadiri	Jan. 2010-Jan. 2011	Oct. 2011-Aug. 2012
6	Mir Anayatullah	May 2010-Nov. 2010	Oct. 2011-Aug. 2012
7	Mohammad Qais	Jan. 2011-Jan. 2012	Oct. 2011-Aug. 2012
8	Mohammad Farooq Amin	Mar. 2011-Apr. 2012	Oct. 2011-Aug. 2012
9	Qazafi Samadi	Mar. 2012-Mar. 2014	Oct. 2011-Aug. 2012
10	Mohammad Hussain Hussaini	July 2012-Jan. 2013	Oct. 2011-Aug. 2012

11	Akhtar Mohammad	July 2012-Jan. 2013	Oct. 2011-Aug. 2012
12	Mohammad Islam Safa	July 2012-Jan. 2013	Oct. 2011-Aug. 2012

The above 12 timeframes of supervision that are listed within the SIV letters Clark allegedly wrote, in which **SUBJECT ACCOUNT #1 and #2** are listed, fall outside the scope of his deployment. In fact, the first six applications above list dates of supervision that precede Clark's deployment. This indicates Clark made false statements in—and falsely verified the contents of—the letters.

35. The veracity of the letters is also undermined by the fact that Clark indicates he was the Contracting Officer Representative ("COR") on the contracts listed within the letters he signed, which is belied by government records that list other individuals as the COR.

36. The veracity of the letters is also undermined by the timing of the wires to Clark shortly before SIV applications linked to Clark were filed according to State Department records:

a. On August 10, 2016, Clark was wired $1,000 twice; over the next two weeks, between August 13 and 20, three applications were filed (Hamidi, Amiri, Qadiri).

b. On September 4, 2016, Clark was wired $953 twice; over the next three weeks, between September 18 and 27, three applications were filed (Amin, Ruhman, Qais).

c. On November 7, 2016, Mir *Enayatullah* wired Clark $1925 twice; two weeks later, Mir *Anayatullah* (possibly the same person) filed his application; over the next few years, five applications were filed (Samadi, Mohammad, Safa, Hussaini, Nazari).

37. Interviews of applicants for whom Pittman and Clark purportedly wrote SIV letters, in which **SUBJECT ACCOUNT #1 and #2** are listed, also undermine the veracity of such letters.

38. As explained above, emails obtained after searching Pittman's email account pursuant to a search warrant issued by this Court reflect that he agreed to sign and verify false SIV letters for applicants in exchange for bribes from Daler, who was the head of an Afghan company, which directly corroborates the allegations in the complaint.

39. Similarly, in March 2021, investigators interviewed Hussaini (see Paragraph 25), for whom Clark signed a letter stating that he was "responsible for Interpreting between all the employees and US citizens and supporting United States Armed Forces" in Afghanistan:

a. Hussaini stated that in 2012 he worked for Raj on a U.S. government project, the Cooper Project, during which time he translated construction terms. When asked why he was not able to interview in English, he answered (in English) that his conversational English was limited, but he understood many construction terms.

b. He stated his supervisor at Raj was the owner, Samadi, and his American supervisor was Clark. He stated he worked for Clark on the Cooper Project in 2012 and he only interacted with Clark on two or three occasions. He also stated he worked for Clark in 2015 (which is belied by the fact that Clark's deployment ended in 2012).

c. He stated that, at Samadi's recommendation, he emailed Clark and asked him to write a SIV letter. He also indicated that he exchanged other emails with Clark (which potentially indicates Clark used **SUBJECT ACCOUNT #1 and #2** to communicate with Hussaini or others during the scheme).

d. Hussaini identified Clark in a picture but denied paying anyone for a SIV letter. He stated his most recent contact with Clark was in or around September 2020 when he had asked Clark to send the original letter, which he showed investigators, and which appears to have been notarized on September 24, 2020.[11]

40. Given that **SUBJECT ACCOUNTS #1 and #2** were listed within the SIV letters, given that they were used to respond to SIV inquiries, given the inconsistent dates of supervision, given the false assertion that Clark was a COR on the contracts, given the timing of wires to Clark, and given Hussaini's limited English, meetings with Clark, and Samadi's advice to contact Clark—all of which is consistent with the complaint—there is probable cause to search such accounts.[12]

---

[11] The notary stamp indicates that the letter was "subscribed and sworn" on September 24, 2020. However, the letter only contains Clark's original signature from October 7, 2018, not a new signature on September 24, 2020. That Clark did not sign the document in the presence of the notary calls the document, and notary stamp, into question. *See* O.C.G.A. § 45-17-8(a)(1) ("Notaries public shall have authority to [] [w]itness or attest signature" of instruments).

[12] In December 2020, the National Visa Center emailed Clark at **SUBJECT ACCOUNTS #1 and #2** and requested verification of the authenticity of the foregoing email accounts. No response was ever received from Clark. Your Affiant further notes that around this time, Clark still had links to Raj, which had obtained a license in July 2020 in which Samadi is listed as President and Clark is listed as Vice President.

b. Afghan Company Letters (SUBJECT ACCOUNTS #3 and #4)

41. In addition to Clark's SIV letters that were used in the scheme, on which **SUBJECT ACCOUNTS #1 and #2** are listed, the SIV applications also contain letters from companies for which the applicants allegedly worked, on which **SUBJECT ACCOUNT #3**, in the case of Raj, and **SUBJECT ACCOUNT #4**, in the case of a company that wrote the most letters, are listed.

42. The complaint's allegation, that Afghan companies sold letters with Clark's letters, potentially taints the letters in which Samadi (Raj) listed **SUBJECT ACCOUNT #3**. Specifically, the complaint alleges that the companies in the schemes, such as Raj, "sell HR [Human Resource Department] letters + Recommend of Clarks to their alliances and families members relatives too."

43. The day after Hussaini's interview, investigators interviewed Samadi, whose statements indicate that he potentially coordinated with Clark in creating fraudulent applications, including the company letter on which **SUBJECT ACCOUNT #3** is listed. Among other things, Samadi stated that he met Clark at Camp Dwyer where Clark was the Contracting Officer Representative for a RAJ contract. He also stated that after the contract ended, they became friends and had several meetings in Dubai. He added that he decided to make Clark his deputy because he thought it would be good for his business to have an American associated with his companies.[13]

44. Clark's relationship with Samadi, along with the other evidence discussed above, further calls into question the SIV applications, including Raj company letters for applicants in which Samadi listed **SUBJECT ACCOUNT #3**.

---

[13] During the interview, Samadi also stated that although he only listed four U.S. government contracts in his own SIV application, he advised his companies were awarded four to six other contracts by the U.S. government. He said he did not list the other contracts because he spent a year in Dubai immediately before he began the application. He also stated that when he returned to Afghanistan, he found his Afghan SIM card (for his phone) was blocked and he could not open his email to get the contract information. Your Affiant has reviewed Samadi's SIV application, including a letter from Raj he signed in which he lists four contracts, and which also lists **SUBJECT ACCOUNT #3**. Your Affiant believes that Samadi's explanation for omitting six contracts (i.e., that he could not obtain information through his phone or email) was potentially false. As the owner of Raj, it appears that he could have likely obtained information about contracts that Raj was awarded through business records. We are investigating the other contracts.

45. That the complaint addresses both the Pittmann SIV scheme—in which there is evidence showing Daler's fraudulent use of the email account that he listed on company letters (Paragraphs 9-16)—and addresses the Clark SIV scheme, potentially indicates Samadi similarly used **SUBJECT ACCOUNT #3** on company letters. As described above, Daler used the email account he listed in company letters to email Pittmann throughout the scheme, including the email that potentially initiated the scheme: "I have been contacted some people they needed a recommendation letter from an American supervisor or engineer or COR. Do you think you can write them a recommendation letter for SIV? They will pay for it."

46. Because the complaint alleges a similar modus operandi with Clark and Raj, your Affiant believes that, like Daler and Pittmann, Samadi's letters in which he listed **SUBJECT ACCOUNT #3** were probably used in the scheme with Clark, an example of which is as follows:

> We found Mohammad Hussain Hussaini as a self-motivated person and he performed sensitive and trusted Activity for the United States Armed Forces . . . [Raj] doesn't have HR Department so May you have any question or query according employment of Mohammad Hussain Hussaini, Please do not hesitate to contact us . . . Qazafi[,] President of RCC[,] **SUBJECT ACCOUNT #3**

47. The fact that Hussaini stated he did not speak much English and only met Clark a few times (Paragraph 39), yet also wired Clark $5,000 (Paragraph 25), not only calls into question Clark's SIV letter, but the whole SIV application, including Samadi's company letter in which he listed **SUBJECT ACCOUNT #3**—particularly because Hussaini stated that Samadi had advised him to contact Clark to obtain a SIV letter (Paragraph 39c).

48. In addition to the fact that Samadi used **SUBJECT ACCOUNT #3** in company letters in the SIV scheme, which is substantially similar to the SIV scheme engaged in by Daler, he also likely used **SUBJECT ACCOUNT #3** when engaging in the procurement fraud scheme.

49. Evidence obtained indicates that Samadi (and Raj) used **SUBJECT ACCOUNT #3** when he emailed U.S. government and military contracting personnel, including Coleman,

about contracts awarded to Raj while Clark and Coleman were deployed (Paragraph 17-29). Because evidence indicates that those contracts were induced by bribes, including $255,000 that Raj wired to LLCs in Georgia that Clark and Coleman set up after their deployments, such evidence also indicates **SUBJECT ACCOUNT #3** was potentially used in the procurement fraud scheme, in addition to the SIV scheme.

50. In addition to the letters that Raj (and Daler) wrote for applicants, the complaint alleges that other Afghan companies conspired with Clark, one of which is associated with Azizullah Afzaly ("Afzaly"), who wrote company letters listing **SUBJECT ACCOUNT #4**:

> Azizullah afzaly whom he is now at the USA he was went by fraud SIV application thru Clark he is now at the USA he met different times Clark at dubai most of the money was paid by Azizullah afzaly in dubai to Clark thru these companies Mr Azizullah just he was get commissions out of this services he did in dubai

51. Records obtained in the investigation show that Afzaly signed the most letters in the scheme with Clark, in which he listed himself as President of a company, and in which he lists **SUBJECT ACCOUNT #4**, an example of which is as follows:

> This is to certify Mr. Mir [A]nayatullah was in employee at afghan us friendship Construction company and he was working as painter at prime contract number W5K9UR-10-7067 Comp Dwyer Afghanistan if you need any further enquiry Regarding His Employment please feel free to contact me at **SUBJECT ACCOUNT #4** . . .
>
> Letter have been signed by Mr[.] [A]zizullah president of aufcc and company HR Department Confirms the employment through this Email: **SUBJECT ACCOUNT #4**

52. Moreover, the format of **SUBJECT ACCOUNT #4** (aufcc.company@gmail.com) is similar to Daler's email account in company letters (sunnycc.company@gmail.com), which Daler used to coordinate with Pittmann in drafting the false SIV letters (Paragraphs 9-16).

53. This is also the same applicant (Mir Anayatullah) who appears to have wired Clark funds only weeks before filing his SIV application (Paragraph 36c), which further undermines the veracity of his SIV application, in which **SUBJECT ACCOUNT #4** is listed.

54. During the timeframe of the scheme, Clark also transmitted wires to Afzaly, which appears to evidence a potential financial relationship, as alleged in the complaint, which further undermines the applications associated with Afzaly, in which he listed **SUBJECT ACCOUNT #4**.

55. Based upon the foregoing evidence and circumstances, there is probable cause to believe **SUBJECT ACCOUNTS #3 and #4** were used in the scheme and contain evidence thereof.

BACKGROUND CONCERNING PROVIDER'S ACCOUNTS

56. PROVIDER is the provider of the internet-based account identified by the **SUBJECT ACCOUNTS**. PROVIDER provides its subscribers internet-based accounts that allow them to send, receive, and store e-mails online. PROVIDER accounts are typically identified by a single username, which serves as the subscriber's default address, but which can also function as a username for other PROVIDER services, such as instant messages and remote photo storage.

57. Based on my training and experience, I know that PROVIDER allows subscribers to obtain accounts by registering on PROVIDER's website. During the registration process, PROVIDER asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate e-mail address for backup purposes, a phone number, and in some cases a means of payment. PROVIDER typically does not verify subscriber names. However, PROVIDER does verify the e-mail address or phone number provided.

58. Once a subscriber has registered an account, PROVIDER provides e-mail services that typically include folders such as an "inbox" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username.

PROVIDER subscribers can also use that same username or account in connection with other services provided by PROVIDER.[14]

59. In general, user-generated content (such as e-mail) that is written using, stored on, sent from, or sent to a PROVIDER account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete an e-mail, the e-mail can remain on PROVIDER's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to exist on PROVIDER's servers for a certain period of time.

60. Thus, a subscriber's PROVIDER account can be used not only for e-mail but also for other types of electronic communication, including**:** instant messaging and photo and video sharing; voice calls, video chats, SMS text messaging; and social networking. Depending on user settings, user-generated content derived from many of these services is normally stored on PROVIDER's servers until deleted by the subscriber. Similar to e-mails, such user-generated content can remain on PROVIDER's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on PROVIDER's servers for a certain period of time. Furthermore, a PROVIDER subscriber can store**:** contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on PROVIDER's servers. Based on my training and experience, I know that evidence of who controlled, used, and/or created a PROVIDER account may be found within such computer

[14] Here, PROVIDER's other services include electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google+ (social networking), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone); and Google Play (which allow users to purchase and download digital content, e.g., applications).

files and other information created or stored by the PROVIDER subscriber. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity.

61. Based on my training and experience, I know that providers such as PROVIDER also collect and maintain information about their subscribers, including information about their use of PROVIDER services. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. Providers such as PROVIDER also commonly have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as PROVIDER typically collect and maintain location data related to subscriber's use of PROVIDER services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.

62. Based on my training and experience, I know that providers such as PROVIDER also collect information relating to the devices used to access a subscriber's account – such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by PROVIDER in order to track what devices are using PROVIDER's accounts

and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI"). Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other PROVIDER accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the PROVIDER account.

63. PROVIDER also allows its subscribers to access its various services through an application that can be installed on and accessed via cellular telephones and other mobile devices. This application is associated with the subscriber's PROVIDER account. In my training and experience, I have learned that when the user of a mobile application installs and launches the application on a device (such as a cellular telephone), the application directs the device in question to obtain a Push Token, a unique identifier that allows the provider associated with the application (such as PROVIDER) to locate the device on which the application is installed. After the applicable push notification service (*e.g.*, Apple Push Notifications (APN) or Google Cloud Messaging) sends a Push Token to the device, the Token is then sent to the application, which in turn sends the Push Token to the application's server/provider. Thereafter, whenever the provider needs to send notifications to the user's device, it sends both the Push Token and the payload associated with the notification (*i.e.*, the substance of what needs to be sent by the application to the device). To ensure this process works, Push Tokens associated with a subscriber's account are stored on the provider's server(s). Accordingly, the computers of PROVIDER are likely to contain

useful information that may help to identify the specific device(s) used by a particular subscriber to access the subscriber's PROVIDER account via the mobile application.

64. Based on my training and experience, I know that providers such as PROVIDER use cookies and similar technologies to track users visiting PROVIDER's webpages and using its products and services. Basically, a "cookie" is a small file containing a string of characters that a website attempts to place onto a user's computer. When that computer visits again, the website will recognize the cookie and identify the same user who visited before. This sort of technology can be used to track users across multiple websites and services belonging to PROVIDER. More sophisticated cookie technology can be used to identify users across devices and web browsers. From training and experience, I know that cookies and similar technology used by providers such as PROVIDER may constitute evidence of the criminal activity under investigation. By linking various accounts, devices, and activity to the same user, cookies and linked information can help identify who was using a PROVIDER account and determine the scope of criminal activity.

65. Based on my training and experience, I know that PROVIDER maintains records that can link different PROVIDER accounts by virtue of common identifiers, such as e-mail addresses, telephone numbers, device identifiers, computer cookies, and names or addresses, that can show a single person group used multiple PROVIDER accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular PROVIDER account.

66. Based on my training and experience, I know subscribers can communicate directly with PROVIDER about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as PROVIDER typically retain records about such communications, including records of contacts between the user and the provider's support

services, and records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

67. In summary, based on my training and experience in this context, I believe that the computers of PROVIDER are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved e-mail for PROVIDER subscribers), as well as PROVIDER-generated information about its subscribers and their use of PROVIDER services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because it can be used to identify the account's user or users. In fact, even if subscribers provide PROVIDER with false information about their identities, that information often nevertheless provides clues to their identities, locations, or illicit activities.

68. As explained above, information stored in connection with a PROVIDER account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a PROVIDER account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by PROVIDER can show how and when the account was accessed or used. For example, providers such as PROVIDER typically log the IP addresses from which users access the account along with the time and date. By determining the physical location

associated with the logged IP addresses, investigators can understand the chronological and geographic context of the PROVIDER account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculpate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the PROVIDER account may indicate its user's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications to conceal them from law enforcement).[15]

69. Based on my training and experience, I know that evidence of who controlled, used, and/or created a PROVIDER account may be found within the user-generated content created or stored by the PROVIDER subscriber. This evidence includes personal correspondence, personal photographs, purchase receipts, contact information, travel itineraries, and other content that can be connected to a specific person or group. In addition, I know that this type of user-generated content can provide crucial identification evidence, whether or not it was generated close in time to the offenses under investigation. This is true for at least two reasons. First, people that commit crimes involving electronic accounts (*e.g.*, e-mail accounts) typically try to hide their identities, and many people are more disciplined in that regard right before (and right after) committing a particular crime. Second, earlier-generated content may be quite valuable, because criminals typically improve their tradecraft over time. That is to say, criminals typically learn how to better

[15] At times, internet services providers such as PROVIDER change the details and functionality of their services. While the information in this section is true and accurate to the best of my knowledge and belief, I have not reviewed every detail of PROVIDER's services in connection with submitting this application for a search warrant. Instead, I rely upon my training and experience and others to set forth the foregoing description for the Court.

separate their personal activity from their criminal activity, and they typically become more disciplined about maintaining that separation, as they become more experienced. Finally, because e-mail accounts and similar PROVIDER accounts do not typically change hands on a frequent basis, identification evidence from one period can still be relevant to establishing the identity of the account user during a different, and even far removed, period of time.

REQUEST TO SUBMIT WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

70. I respectfully request, pursuant to Rules 4.1 and 41(d)(3) of the Federal Rules of Criminal Procedure, permission to communicate information to the Court by telephone in connection with this Application for a Search Warrant. I submit that Trial Attorney Matt Kahn, an attorney for the United States, is capable of identifying my voice and phone number for the Court.

CONCLUSION

71. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on PROVIDER, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

/s/ Kevin Naylon
Kevin Naylon
Special Agent
Special Inspector General for Afghanistan Reconstruction

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Oct 29, 2021
Time: 3:13 PM, Oct 29, 2021

Hon. Andrea K. Johnstone
United States Magistrate Judge

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with the PROVIDER accounts identified by orlandoclark8@gmail.com, wmsconstructiondesign@gmail.com, raj.wafi@gmail.com, and aufcc.company@gmail.com, which are stored at premises owned, maintained, controlled, or operated by Google, LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized and Procedures to Facilitate Execution of the Warrant

I. Information to be disclosed by PROVIDER to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of PROVIDER, including any records that have been deleted but are still available to PROVIDER, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), PROVIDER is required to disclose the following information to the government corresponding to each account or identifier ("Account") listed in Attachment A:

a. The contents of all emails associated with the Account from January 1, 2011 to the present, including stored or preserved copies of emails sent to and from the Account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the Account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the Account was created, the length of service, the IP address used to register the Account, log-in IP addresses associated with session times and dates, Account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank Account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the Account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the Account, including contacts with support services and records of actions taken.

The PROVIDER is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant via U.S. mail, courier, or e-mail to the following:

Special Agent Kevin Naylon
Special Inspector General for Afghanistan Reconstruction
1550 Crystal Drive, 9th Floor
Arlington, VA 22202
kevin.j.naylon.civ@mail.mil
703-731-5540

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 201 (Bribery), § 371 (Conspiracy), § 1001 (False Statement), § 1343 (Wire Fraud), § 1546 (Visa Fraud), § 1956 (Money Laundering), and 31 U.S.C. § 5324 (Structuring), as described in the affidavit submitted in support of this Warrant, including, for each Account, information pertaining to the following matters:

(a) Evidence indicating any individual, company or agent thereof, offered or promised to give anything of value to any public official, including but not limited to a U.S. government employee or U.S. government contractor involved with the process of reviewing or soliciting bids or awarding contracts;

(b) Evidence indicating any public official, including but not limited to a U.S. government employee or U.S. government contractor involved with the process of reviewing or soliciting bids or awarding contracts, sought to receive from any individual, company or agent thereof, anything of value;

(c) Evidence indicating any public official improperly exercised influence in attempting to award U.S. government or military contracts;

(d) Evidence indicating any individual, company or agent thereof, falsified or concealed any information, or made any false, fictitious or fraudulent statement, in documents submitted to the U.S. government, including but not limited to documents in support of U.S. government or military contracts and documents in support of visa applications;

(e) Evidence indicating that individuals drafted fraudulent documents, including documents in support of visa applications, as well as evidence indicating individuals conspired to engage in the foregoing activity;

(f) Evidence indicating that individuals sent or received or sought payments for drafting or signing or otherwise assisting with the creation of fraudulent documents, including documents in support of visa applications;

(g) Evidence indicating that any individual, corporation or agent thereof, conducted any financial transaction involving the proceeds of unlawful activity, or concealed or disguised the nature of the proceeds of unlawful activity, or attempted to structure a transaction so as to avoid a transaction reporting requirement;

(h) Information that constitutes evidence of the identification or location of the user(s) of the Accounts;

(i) Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted the commission of the activity under investigation; or (ii) communicated with the Account about matters relating to the activity under investigation, including records that help reveal their whereabouts;

(j) Information that constitutes evidence indicating the Account user's state of mind related to the criminal activity under investigation;

(k) Information that constitutes evidence concerning how and when the Account was accessed or used, to determine the geographic and chronological context of access, use, and events relating to the crime under investigation and to the Account user;

(l) Information sufficient to identify any co-conspirators and other participants in the scheme and related to any attempts to conceal the scheme.